DoD Information Technology Security Certification and Accreditation Process

Information Assurance Program Management Office

Agenda

- Background
- Status
- Support
- Way Ahead
- Questions

Background

Information Assurance

Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

Background

Authority and Status

- **ASD/C3I Memo 19 Aug 92**
  - **Develop Standardized C&A Process**
- **DITSCAP/DoD Instr 5200.40**
  - **OSD formal coordination May 97**
  - **ASD Signature 30 Dec 97**
  - **Provides high level “process” details**

DITSCAP

- DoD Information Technology Security Certification and Accreditation Process
- Defines a process for uniform practice of C&A
- Addresses life cycle approach
- Infrastructure-centric approach
- Describes generic process activities and tasks
- Implementation details are provided through established C&A environment

DITSCAP

Benefits

- **Establishes a standard C&A process**
  - **Standardizes security activities and documentation**
  - **Identifies 4 levels of certification analysis**
- **Process is applicable regardless of lifecycle**
- **Process applies to any type acquisition strategy or development**

DITSCAP

Benefits

Previous DISA Documentation Requirements

- SSP
- Concept of Operations
- System User's Guide
- CMP
- Contingency Plan
- MOA(s)
- ST&E Plan, Procedures and Report
- SOPs
- Architecture

Reduces Documentation Requirements

DAA/PM/USER/CA

DITSCAP

Definition

Mission, Architecture & Environment
Security Requirements
SSAA

Verification

Security Features Implemented
Documentation

Validation

Validate the integrated system

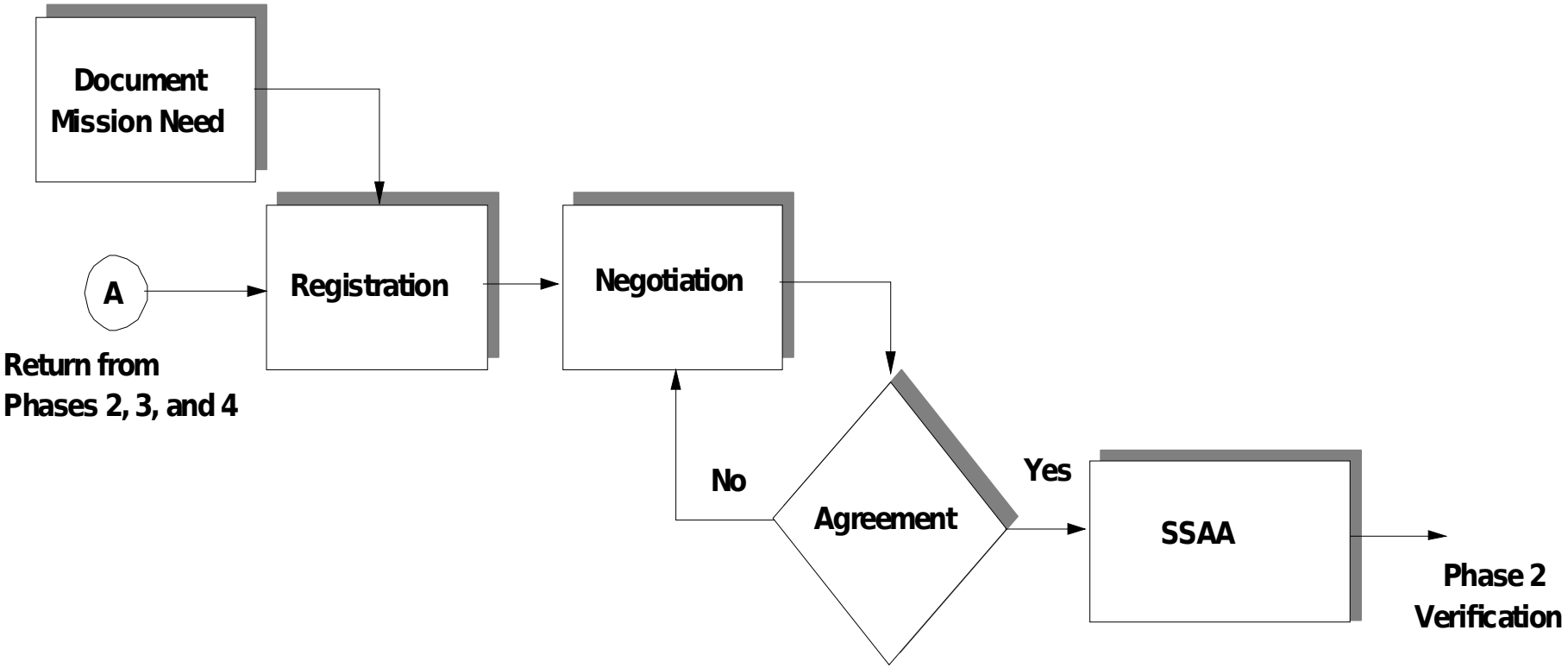
Post Accreditation

Monitor compliance and change management

Security Life Cycle

Success-oriented Certification and Accreditation Process

Phase 1: Definition



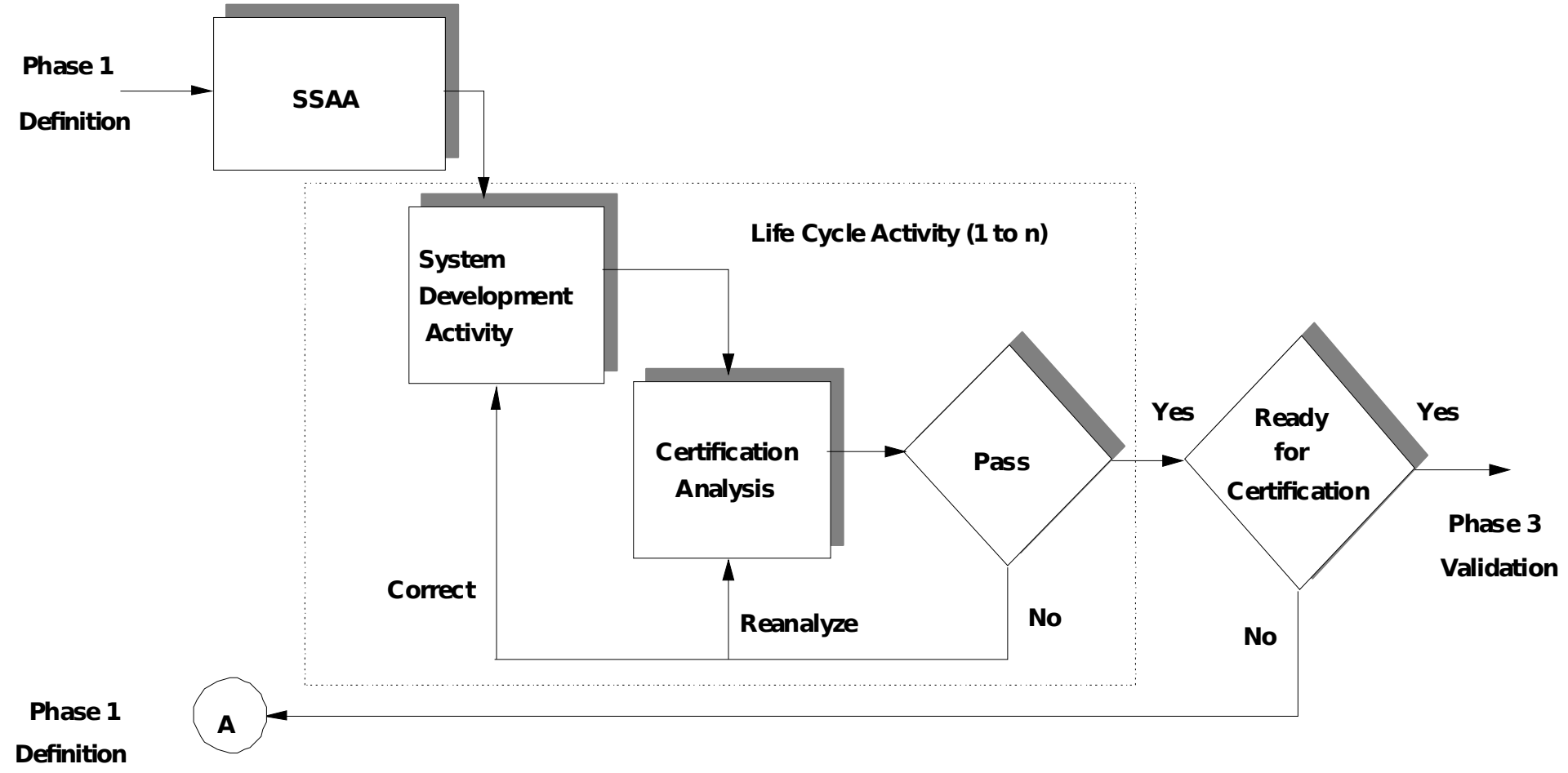
Phase 1, Definition

- Phase 1, Definition: Initiates the DITSCAP process by acquiring or developing the information necessary to understand the IT and then using that information to plan the C&A tasks.

Phase1(Tasks)

- Task 1: Prepare the Mission Description and System Identification
- Task 2: Register the System
- Task 3: Prepare the Environment and Threat Description
- Task 4: Prepare the System Architecture Description
- Task 5: Determine the ITSEC System Class
- Task 6: Determine the System Security Requirements
- Task 7: Identify the C&A Organizations and the Resources Required.

Phase 2 : Verification



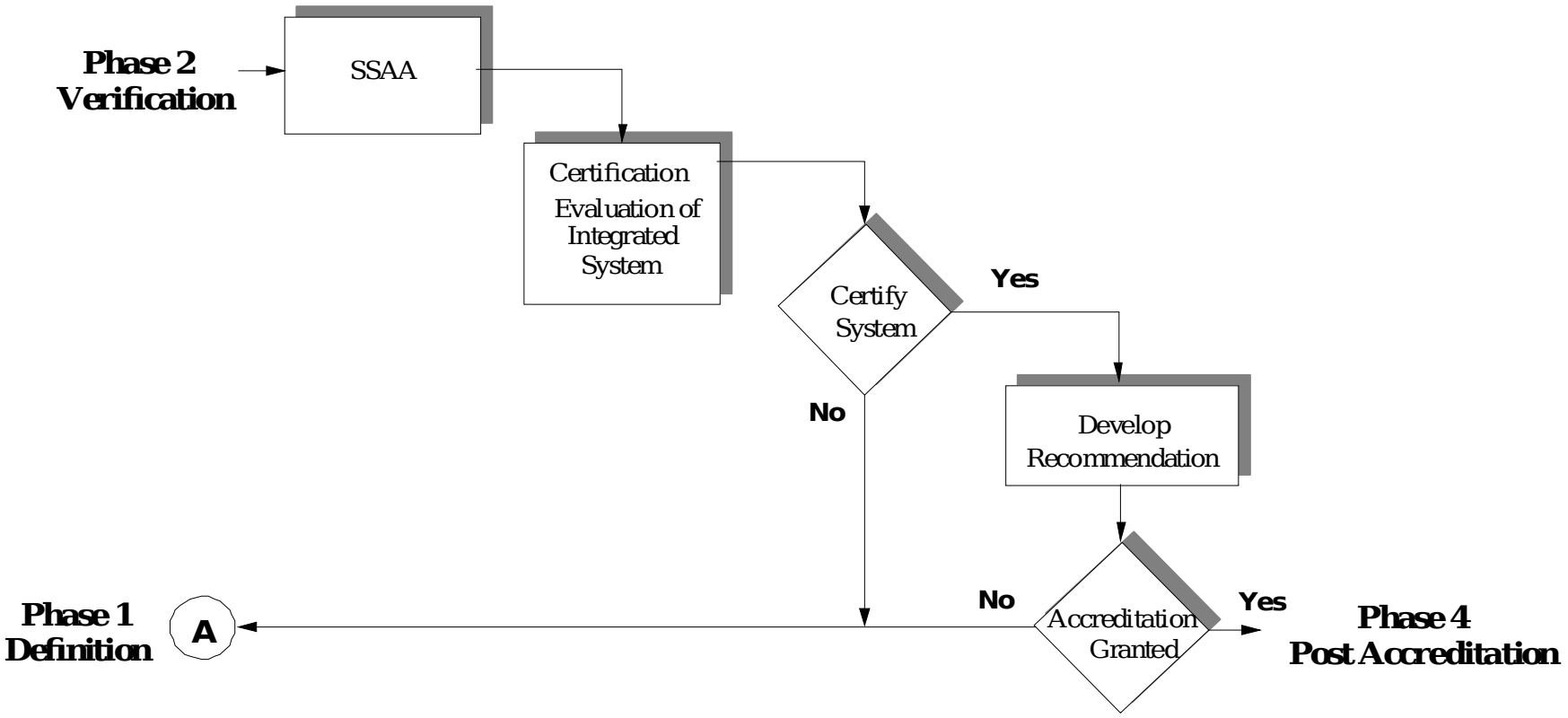
Phase 2, Verification

- Phase 2 is to verify the system's compliance with the requirements agreed on in the SSAA. The goal is to obtain a fully integrated system for certification testing and accreditation.

Phase 2 (Tasks)

- Task 1: System Architecture Analysis
- Task 2: Software Design Analysis
- Task 3: Network Connection Rule Compliance Analysis
- Task 4: Integrity Analysis of Integrated Products (COTS, GOTS, Non-Developmental Item)
- Task 5: Life-Cycle Management Analysis
- Task 6: Vulnerability Assessment

Phase 3: Validation



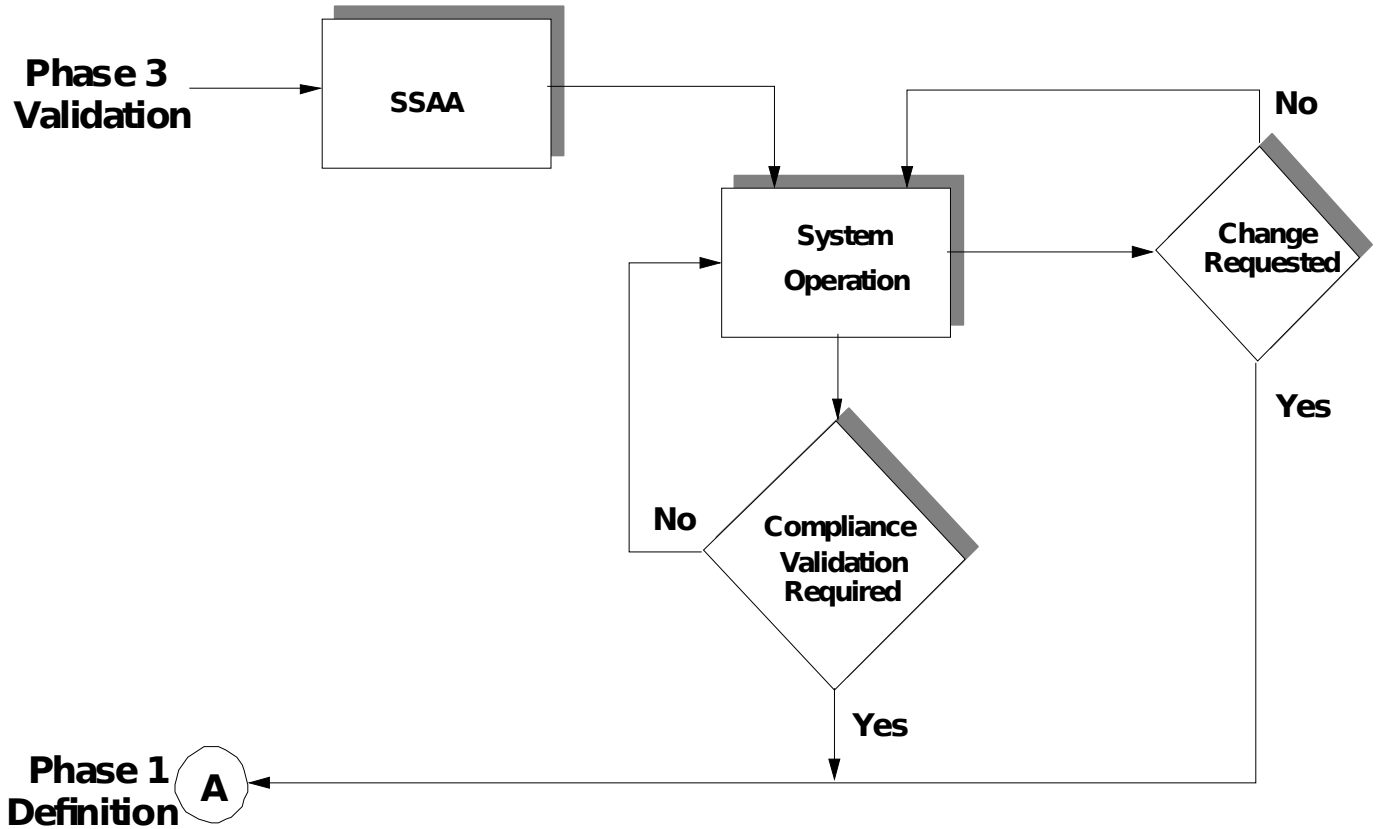
Phase 3, Validation

- Phase 3, Validates the fully integrated system compliance with the requirements stated in the SSAA. The goal is to obtain full approval to operate the system - accreditation.

Phase 3 (Tasks)

- Task 1: Security Testing and Evaluation
- Task 2: Penetration Testing
- Task 3: Verify TEMPEST Compliance (only if TEMPEST applies)
- Task 4: Verify Appropriate Use of COMSEC Material and Equipment (only if COMSEC applies)
- Task 5: System Management Analysis
- Task 6: Site Accreditation Survey
- Task 7: Contingency Plan Evaluation
- Task 8: Risk Management Review

Phase 4
Post Accreditation



Phase 4, Post Accred

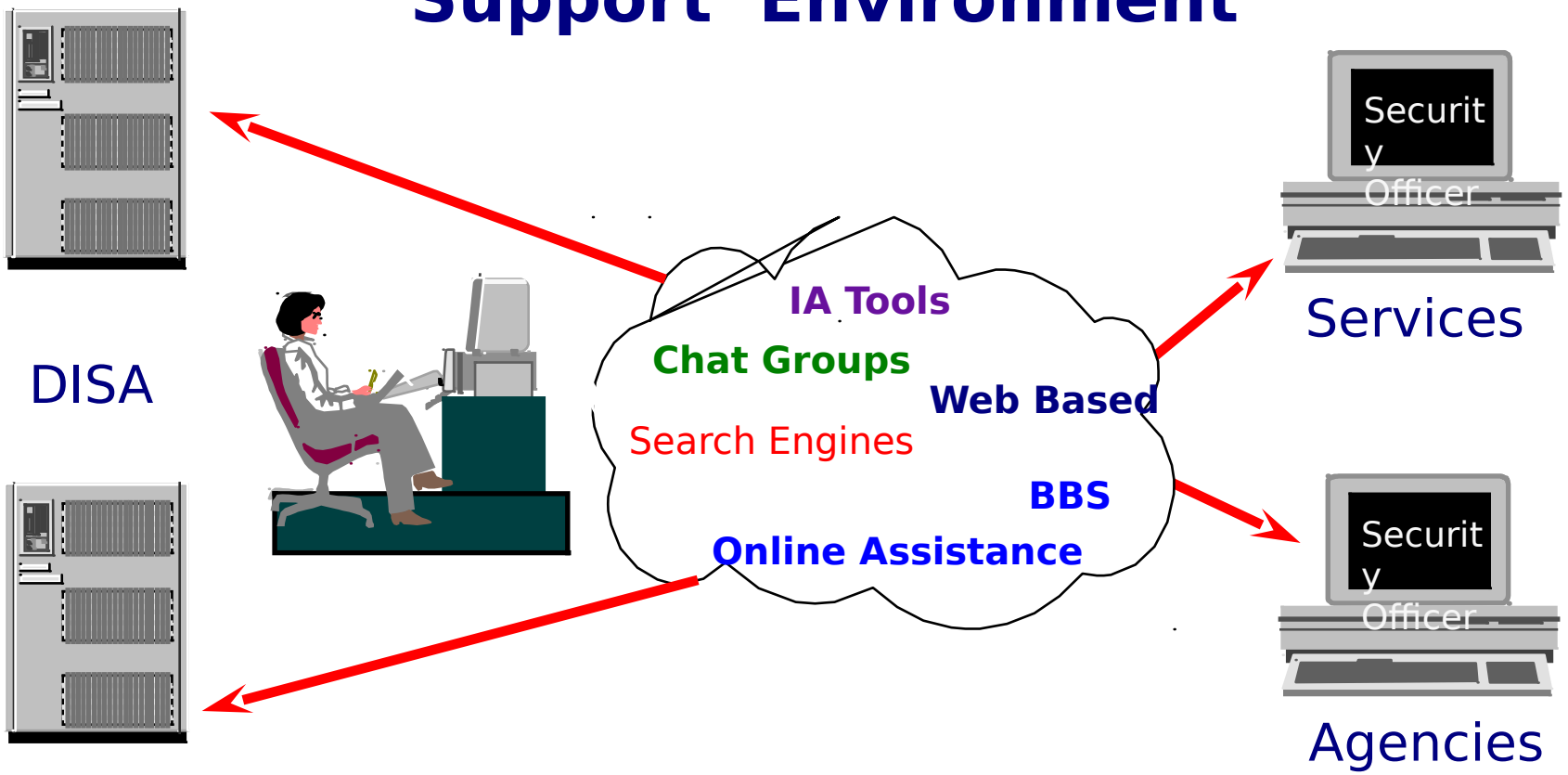
- Phase 4 begins after the system has been certified and the site accredited for operations. This phase continues until the information system is removed from the service, a change is planned for the system, or a periodic compliance validation is required.

Phase 4 (Tasks)

- Task 1: SSAA Maintenance
- Task 2: Physical, Personnel and Management Control Review
- Task 3: Contingency Plan
- Task 4: Verify TEMPEST Compliance (only if TEMPEST applies)
- Task 5: Verify Appropriate Use of COMSEC Material and Equipment (only if COMSEC applies)
- Task 6: Change Management
- Task 7: Conduct Risk Management Analysis

Implementation Approach

Information Assurance Support Environment



Information Assurance Support Environment

- Provides online information on various aspects of INFOSEC

One stop shop for Security

- Technology allows for exchange among wide variety of participants

Information Assurance Support Environment

- Provides detailed steps of certification activities to support PMOs, Security Staff, and onsite ISSOs/ISSMs
- Provides online assistance
- Reduces cost associated with Certification and Accreditation
  - Automates processes
  - Promotes reuse
  - Reduces documentation requirements

Information Assurance Support Environment

- Web-based DOD Help Environment for Information Assurance professionals

- Functional Areas
  - ETA
  - SABI/MLS
  - DITSCAP
  - Policy
  - C&A/ST&E
  - ITSC Contract
  - Tools
  - PKI

IASE Features

- Person to receive request/provide information requested
- Request for Information Ticket System
- Frequently Asked Questions (FAQ)
- Solutions Database
- Chat/Discussion Rooms
- Whiteboard
- Mail List
  - Subscriptions
  - By Topic
- Bulletin Board System
- “Search our Site”

IASE Access

- Unclassified Site:
  - NIPRNet: .mil and .gov accounts required
  - URL: *http://iase.disa.mil/*
  - Information Desk Unclassified E-Mail: *IASE@ncr.disa.mil*
- Classified Site also available
- Hours of Operation:
  - Telephone: 703-681-IASE
  - Information Desk: M-F, 7:30a-4:30p
  - IASE Web Site: 24 x 7

Status

- **DITSCAP Annual Review**
  - **Allows for a living document**
- **Application Guide**
  - **Completed informal staffing**
  - **In OSD Formal 106 process**
  - **Expected to become DOD Manual**

Status (cont'd)

- C&A Working Group
  - Purpose
  - Bi-monthly meetings
- National Agencies
  - NSTISSC C&A Subgroup
  - NIACAP

Support

- **IASE**
  - Allows community to standardize approaches
  - On-line access to documents
  - Chat rooms
- **SSAA Template**
  - Currently in Development
  - Goal is a “Turbo Tax” version
- **Others**
  - C&A Working Group explores ideas
    - Review tools (i.e. NSA, Risk Management, etc)

Way Ahead

- **Business Case**
- **Executive Summary**
- **Standardized Brief**
- **Application Document**
- **Accreditor’s Guideline**
- **Merge with Fed/Civil Agency processes through NSTISSC**
- **Provide IA tools to assist the community**
- **Requirements Database**

Summary

- **Certification and Accreditation is the critical “protect” element IA model**
- **Interconnected-Interdependent nature of DoD Mission requires network-centric Accreditation Process**
- **Implement process across DOD and merge with Fed and Civil Agencies**
- **Online support environment provides assistance and guidance**

QUESTIONS

BACK-UP SLIDES

Back-up

Policy